CYBER SECURITY
THE ESCALATING LANDSCAPE

Fred Dumas, Chairman, Dark Cubed

payCLT dark3

Agenda

- The Cyber Threat Landscape for Banking and Payments
  - Securing Transactions
  - The Threat Surface is changing
- The Cyber Security Marketplace is broken
- Cyber Crime has never been easier, or more profitable
- The value of shared information
- Introducing Dark Cubed

payCLT

In 2016 "**cybercrime cost the global economy over $450 billion**, over 2 billion personal records were stolen and in the U.S. alone over 100 million Americans had their medical records stolen," said Steve Langan, chief executive at Hiscox Insurance, told CNBC

dark3

Cost is rising

Financial Services has led the way in Security

- Synchronous Passwords
- Biometrics
- Out of Band Authentication
- Pattern Analysis
- Encryption
- Digital Signatures

Risks are Changing

Protecting the TRANSACTIONS is not enough

Your NETWORK

Your SUPPLY CHAIN

Your CUSTOMERS

Your Network

- 3,000 Personal Computers' hard drives wiped clean
- 50% of servers wiped clean
- 7,000 employees paid by paper check
- Paper memos and Fax machine
- Confidential Salary Information
- 47,000 Social Security Numbers
- Tens of millions in lost profits

Your Supply Chain

- HVAC Vendor was the initial access point
- 40,000,000 customer accounts hacked
- $420,000,000 in lost profits to Target

Your Customers

THE DENVER POST

BUSINESS › TECHNOLOGY

60% of small companies that suffer a cyber attack are out of business within six months.

Simple steps can help you avoid a hack that could destroy your fortunes

By **GARY MILLER** | GEM Strategy Management

PUBLISHED: October 23, 2016 at 12:01 am | UPDATED: March 24, 2017 at 12:29 pm

- The Ponemon Institute reports that the average cost to remediate a hack is $690,000 for a small business, and over $1 million for a mid market company.
- As banks, you have a vested interest in your customers' financial health, so THEIR CYBER SECURITY SHOULD BE IMPORTANT TO YOU!

The Problem with Cyber Security Today

- Products are built for the largest, most sophisticated companies
- Today's products assume that the buyer has budget, and talented resources

JAN 27, 2016 @ 07:15 AM 9,802 VIEWS

Bank of America's Unlimited Cybersecurity Budget Sums Up Spending Plans In A War Against Hackers

Forbes

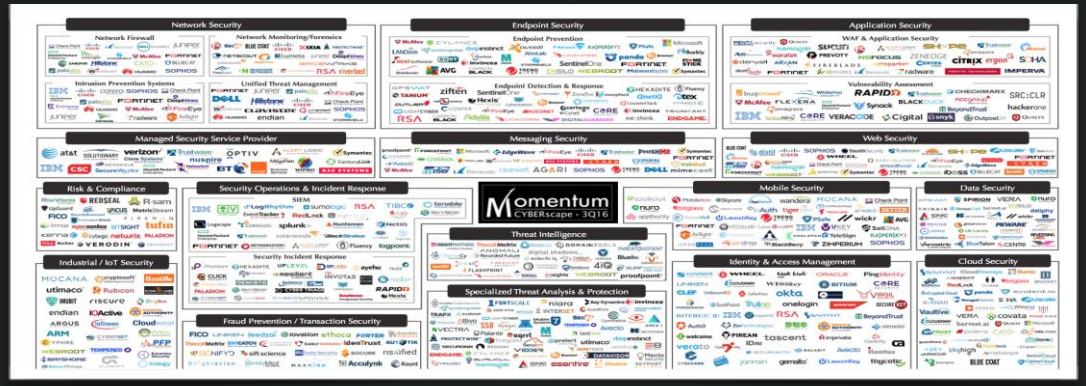
Steve Morgan, CONTRIBUTOR

I write about the business of cybersecurity. FULL BIO

Opinions expressed by Forbes Contributors are their own.

The U.S. federal government, big banks, and big businesses are spending big bucks in a war against hackers and cyber criminals.

In a live interview from Davos Switzerland on Bloomberg roughly one year ago, Bank of America Corp. CEO Brian Moynihan said the nation's second largest lender would spend $400 million on cybersecurity in 2015... and it was the first time in 20 years of corporate budgeting he had overseen a business unit with no budget. Moynihan said the only place in the company that didn't have a budget constraint was cybersecurity.



- Mid sized companies are overwhelmed by choice, complexity and cost
- Most companies are unable to afford, install or operate the products available today

Unfair Fight

PenTesting
Ethical Hacking

Cyber Crime

Port Scanning, Network Monitoring, Password Hacking. These tools are all free and open source. They are used by the good and bad guys.

We need to establish a common understanding between the geeks and the executives so we can begin to collaborate on solutions.

dark3

Understanding the Scale

Assets	Number of Banks / Credit Unions
Greater than 1 Trillion in Assets	4
100 Billion - 999 Billion	22
50 Billion - 99 Billion	13
25 Billion - 50 Billion	22
1 Billion - 24 Billion	677
500 Million - 999 Million	662
100 Million - 499 Million	2,954
Under 100 Million	5,000+

Where To Go From Here…

Invest

Organizations need to understand their role in managing organizational risk AND systemic risk

Share

Information sharing must occur at speeds that we are not capable of today.

Adjust

We are never done with security, the key is to remain flexible and keep adjusting

dark3

Invest

Top three investments that MUST happen today (if you haven't already invested):

1) **Logging Infrastructure:** Collect information about your network
2) **Monitoring Infrastructure:** Know when things are changing
3) **Detection Infrastructure:** Have the ability to detect the most common threats, these are canaries in the coal mine.

Share

Nobody has enough resources, so we must share and collaborate:

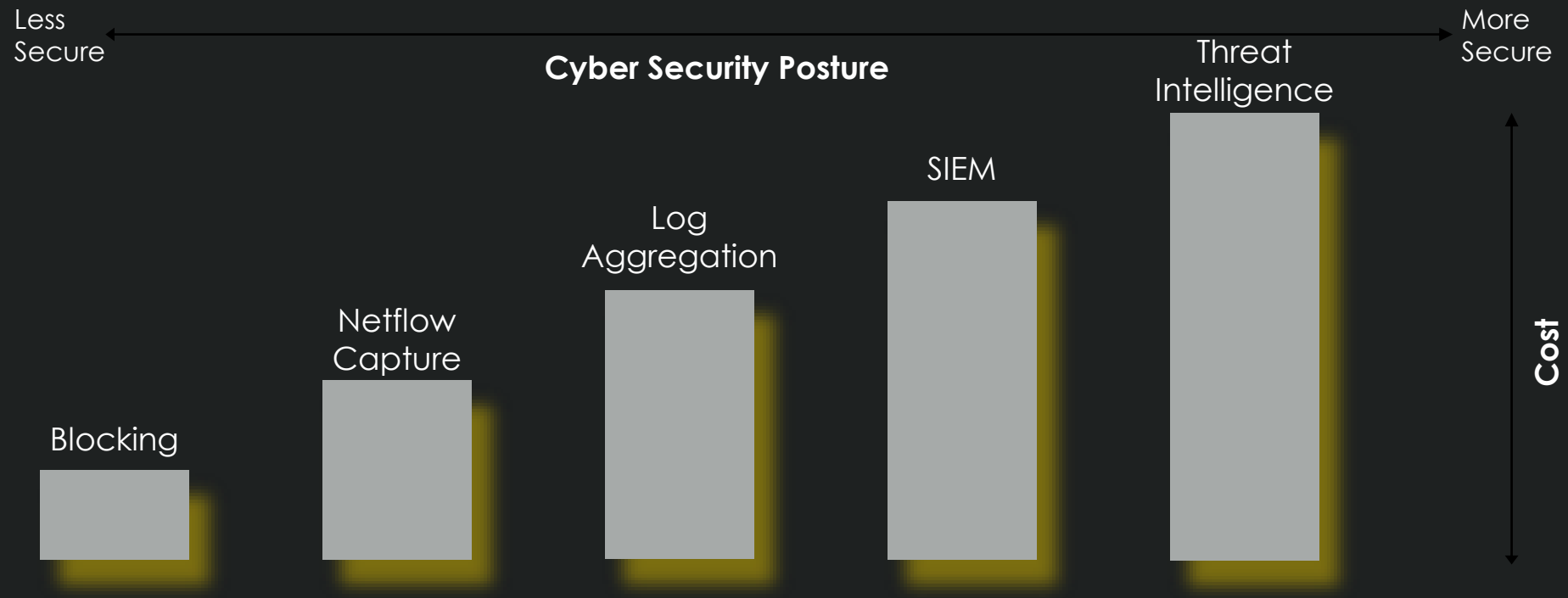
1) **Known Attacks:** Attack against one of us is an attack on everyone
2) **Suspected Attacks:** Leading indicators of future problems
3) **Efficacy of Protection Approaches:** We are stronger when we work together.

Adjust

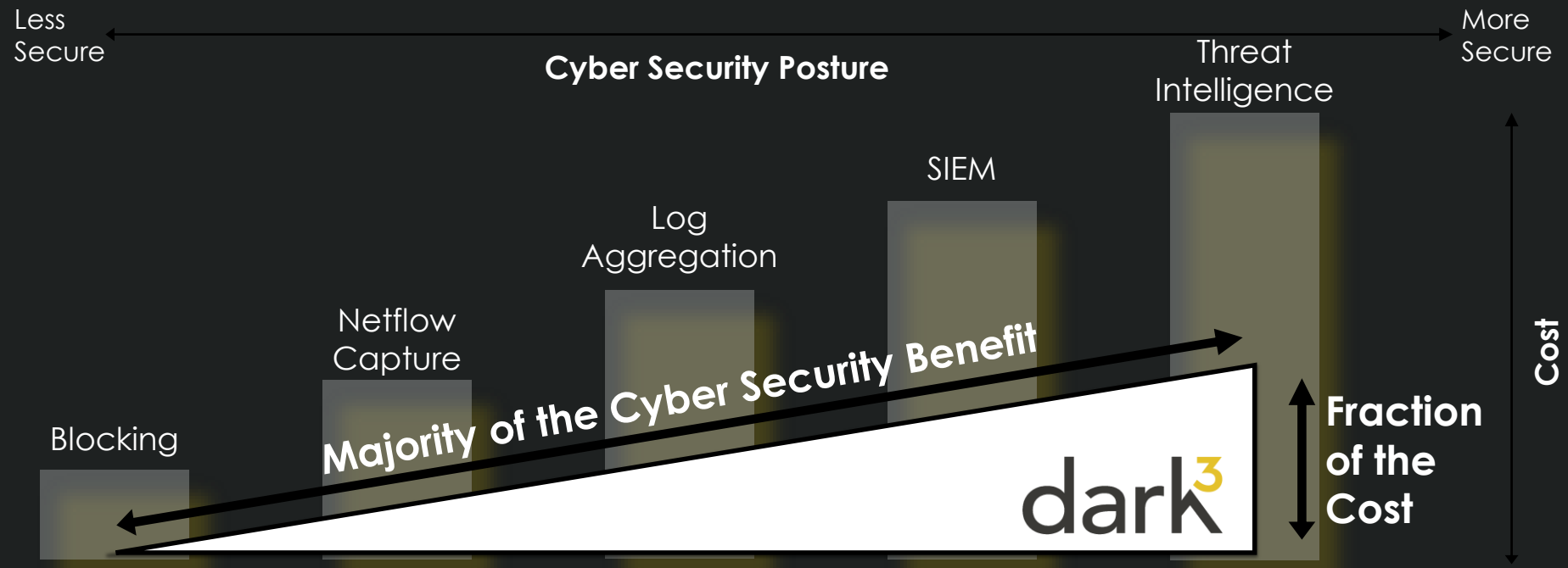
We are never "done" with security, keep in mind the following key factors:

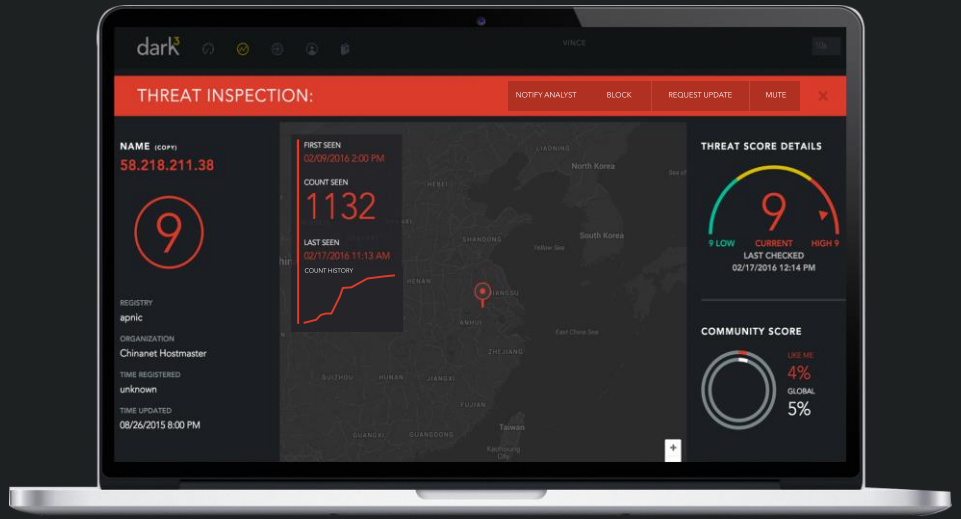
1) **Intelligent Adversaries:** We are fighting brilliant adversaries that are very creative in developing new ways to attack our infrastructures.
2) **They Use The Same Tools:** The bad guys buy the same security tools we use so they know they can defeat them.
3) **Right Once:** The attacker only needs to be right one time, we need to be right every time.

Market Fit


Less Secure
Cyber Security Posture
More Secure
Blocking
Netflow Capture
Log Aggregation
SIEM
Threat Intelligence
Cost

Market Fit


Less Secure
Cyber Security Posture
More Secure
Blocking
Netflow Capture
Log Aggregation
SIEM
Threat Intelligence
Majority of the Cyber Security Benefit
dark3
Fraction of the Cost
Cost



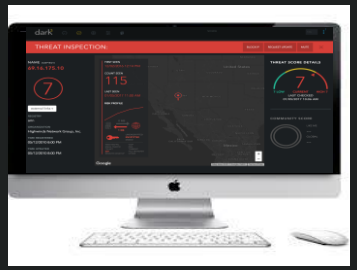
"Any intelligent fool can make things bigger, more complex...It takes a touch of genius — and a lot of courage to move in the opposite direction."

Ernst F. Schumacher

dark3

Architecture

Dashboard



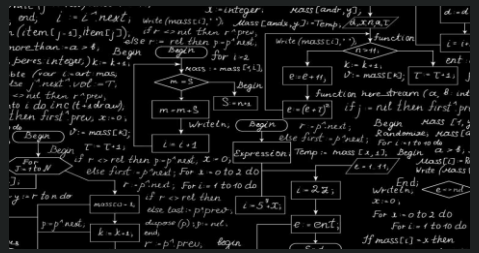
- *View high risk connections*
- *Block traffic with one click*
- *Set alert / auto-block preferences*

Appliance

- *Monitors your Network*
- *Database of Historic Threat Scores*
- *Powers the Dashboard*

Your Network

Threat Scoring Engine



- *60+ sources of Threat Intelligence*
- *Predictive Analytics*
- *Community Scoring*

Black Box

- *List of popular threat scores*
- *Provides scale and anonymity*

Dark Cubed Operations Center

Features

- ✓ Real Time Monitoring
- ✓ Threat Intelligence
- ✓ Elegant User Interface
- ✓ Simple Workflow
- ✓ Active & Automatic Blocking

Threat Inspection

Executive Report

Customer Success Stories

Unnamed National Health Care Company

National Organization with over 50 Regional Centers and over 600 clinics

1776 FINANCIAL

Independent Financial Advisor with over five hundred million in assets under management

LIVE OAK BANK

#2 SBA Loan Originator in the US.

ACPS ALEXANDRIA CITY PUBLIC SCHOOLS

School district with 15 schools and over 15,000 students

DISCOVERY PLACE SCIENCE

Charlotte NC based company operates science, nature and kids museums.

GROUP NIRE Renewable Energy Solutions

Texas company that field tests Renewable energy solutions

Experienced Leadership Team

Vince Crisler, CEO / Co-Founder

20+ years experience. Air Force Officer, White House Communications Agency, Pentagon, and White House CISO, 6+ years supporting National Security Staff and Department of Homeland Security protecting Federal Government and Critical Infrastructure from Cyber threats.

Keith Schwalm, COO
20+ years experience, to include United States Secret Service, Director on the President's Critical Infrastructure Protection Board, and founding portfolio manager of the Science and Technology Directorate at DHS.

Matt Ellis, VP Sales & Marketing
25+ years of Sales and Product Management experience, leadership positions at ACI Worldwide, Clear2Pay, S1 and Bank of Boston. Successful exit of over $500M at Clear2Pay.

Bryan Richardson, CTO
Managed large-scale cyber modeling and simulation at Sandia Labs. Responsible for cyber R&D relationships with USAF, OSD DO T&E, NORAD/NORTHCOM, and CYBERCOM. Offensive Security Certified Professional.

QUESTIONS?

dark^3

info@darkcubed.com